UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,779	03/14/2002	Todd Weston Arnold	AUS920010984US1	4841

40412 7590 07/12/2006

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 07/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 10/099,779	Applicant(s) ARNOLD ET AL.	
	Examiner Jeffery Williams	Art Unit 2137	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 19 June 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☒ The Notice of Appeal was filed on *6/5/06*. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,6-8,14 and 19-29*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:

    _____.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, 7, 8, 14, 19, 20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan, "Method and Apparatus for Encoding Keys", U.S. Patent, 6,549,626 in view of Hosokawa, "Internet Broadcast Billing System", U.S. Patent Publication, 2001/0023416 A1.

Regarding claim 1, Al-Salqan discloses:
receiving, at a security module, a first password corresponding a software application (Al-Salqan, col. 2, lines 12-28, 49-63; fig. 2, elem. 204); generating, at a security module, a first mask value based on the first password (Al-Salqan, col. 4, lines 29-46; fig. 2); combining, at a security module, the first mask value with a first encryption key (Al-Salqan, col. 4, lines 49-52; fig. 2);
encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key (Al-Salqan, fig. 2). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).
returning the encrypted tied key to the software application (Al-Salqan, fig. 2, elem. 246). Al-Salqan discloses the returning of the encrypted tied key to what is termed the "user". Clear to those of ordinary skill in the art, the term "user" is a reference to a user employing a computer-implemented application, an interface to the security module. For understanding of such, the applicant's representative is respectfully invited to consider the Applicant's own disclosure of the prior art, which evidences that which was clear to those having knowledge of technology (Spec. pg. 1, lines 16-17, 22-24; pg. 2, line 27 – pg. 3, line 2). Herein, the Applicants clearly equate, viewing as interchangeable, a customer (a "human") with an application, meaning, more specifically, that a human does not interact with the computer system as he/she would interact with another human, but instead, interacts with the computer system via an application. Thus, when one of ordinary skill in the art refers to a "customer" as using an encryption key within a computer system, in actuality, that one is appropriately and reasonably referring to an "application" in employment by a user. Al-Salqan discloses a computer software security module as outputting an electronic key to a "user" via an output, the key subsequently used by the user (fig. 2, elem. 246). In harmony with the understanding of those having technical knowledge, and in a manner similar to the applicant's themselves, Al-Salqan discloses a user utilizing a computer-implemented application to encrypt data, an thus a key being provided to an application (Al-Salqan, col. 3, lines 16-52).
determining, at the software application, that the encrypted tied key corresponds to the security module; in response to the determining, sending the encrypted tied key and a second password form the software application to the security module over a computer network, the second password being the same as the first password (Al-Salqan, fig. 3, elems. 302,306). Herein, Al-Salqan discloses the transmission of a encrypted tied key and password within an interconnected group of computing elements. The examiner would like to point out that the limitation determining, at the software application, claimed within a method comprising steps, does not indicate who or what does the determining and how such a determination is conducted. Furthermore, the examiner takes note that the claim vaguely claims a correspondence between a key and module, but provides no indication of what comprises the correspondence. Al-Salqan discloses the above limitations, as the correct password and a corresponding tied key of a user is passed to the security module via the software means for enabling such interaction between the user and security module (Al-Salqan, col. 3, lines 16-52).
receiving, at the security module, the encrypted tied key and the second password from the software application; in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key (Al-Salqan, fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).
generating a second mask value based on the second password (Al-Salqan, col. 4, lines 29-46; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05);
separating a recovered encryption key from the recovered tied key using the second mask value (Al-Salqan, col. 7, lines 45-49; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teaching of the recovery of an recovered encryption key from the recovered tied key ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).
and encrypting data provided by the software application using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 1, lines 21-28; col. 7, lines 48,49; col. 3, lines 52-56). First, regarding the limitation "provided by the software application", the examiner notes that such is descriptive language describing data. This has added no further structure to the claim, the data itself being non-functional descriptive material. Additionally, the examiner points out that the above-mentioned limitation provides no indication as to how the software provides data to be encrypted or to what or whom the software provides the data to be encrypted. Al-Salqan discloses the encryption of symmetric encryption keys. Al-Salqan discloses that keys, when they are requested and obtained by the user, are used to encrypt data (Al-Salqan, col. 3, lines 55-57; col. 7, lines 48-49). When an encryption key becomes lost, an authorized user of the key may recover the key for use again (Al-Salqan, col. 1, lines 61-65) Al-Salqan discloses that such symmetric encryption keys are used to encrypt and decrypt data, and for such, an application of software is used (Al-Salqan, col. 1, lines 61-65; col. 3, lines 16-52).

Al-Salqan discloses a system designed to ensure the secrecy of a data encryption key, such as a symmetric key. Secrecy is accomplished by encrypting the data encryption key. However, though Al-Salqan discloses enabling the secrecy of a symmetric data encryption key, it does not disclose the enabling of the authenticity of the key. Thus, Al-Salqan does not disclose wherein the first "encryption key" is derived from a generated key and a known value the combining resulting a tied key or that the recovered "encryption key" includes a recovered generated key and a recovered known value.
Hosokawa discloses a method for the verification of the authenticity of a data-encryption key, the method being performed "as a security

measure" (Hosokawa, par 37). This "security measure" of ensuring authenticity is additional to the security measure of ensuring secrecy - encrypting the data encryption key. The method comprises the creation of a "tied key", or an "encryption key" derived from a generated key and a known value (Hosokawa, par. 32, lines 8-12; par. 33, lines 1-5; par. 37, lines 11-13; par. 44, lines 11-18). Hosokawa attaches a "known value", a digital signature, to generated key, and thereby creates a "tied key". After the "tied key" is decrypted, the attached digital signature is compared to an authentic digital signature so as to verify the authenticity of the generated key. If authentic, the generated key is used for encrypting data. Thus, Hosokawa discloses a method usable to verify the authenticity of an encryption key, the method ensuring a measure of security.
It would have been obvious to one of ordinary skill in the art to combine the method of Hosokawa with the system of Al-Salqan. This would have been obvious because one of ordinary skill in the art would have been motivated to enhance the security of the system of Al-Salqan, by not only enabling the secrecy of the data encryption key, but also the authentication of the data encryption key. Thus, a more secure system is provided.

Regarding claim 6, the combination of Al-Salqan and Hosokawa disclose:
determining whether the recovered known value is correct; and processing a data file based on the determination (Hosokawa, col. 2, pars. 32, 33; Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 7, the combination of Al-Salqan and Hosokawa disclose:
wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 22, the combination of Al-Salqan and Hosokawa disclose:
wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted (Hosokawa, par. 41). The combination of Al-Salqan and Hosokawa disclose that the key is appropriately used for securing data, thus the key is at a level of security suitable for securing sensitive data.

Regarding claims 8, 14, 19, and 20, they are the system means and computer program product claims implementing the method of claims 1, 6, and 7, and they are rejected, at least, for the same reasons. Further, regarding claim 8 specifically, it is rejected because the combination of Al-Salqan and Hosokawa disclose:
one or more processors; a memory accessible by the processors; one or more nonvolatile storage devices accessible by the processors; a hardware security module accessible by the processors; a data security tool for securing data using the hardware security module (Al-Salqan, figs. 1, 2; col. 3, lines 16-45).

Claims 21, 23, 24, 26, 27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Al-Salqan and Hosokawa in view of the Applicant's Admitted Prior Art.

Regarding claims 21 and 23, the combination of Al-Salqan and Hosokawa does not disclose wherein the security module is a separate hardware security module and wherein encrypting the data is performed within the security module. However, it would have been logical to one of ordinary skill in the art employ a security module to provide security to data. Furthermore, it would have been logical to one of ordinary skill in the art to utilize hardware versus software, as hardware is known to provide advantages in security and performance. The applicants, themselves, attest to the above facts in their disclosure of the known prior art. The applicants have admitted that prior art comprises the use of hardware security modules and that the hardware security modules are useable for encrypting data that a user desires to be secured (Spec., page 2, pars. 1 – 3).
It would have been obvious to one of ordinary skill in the art to employ the prior art teachings disclosed by the Applicants within the combination of Al-Salqan and Hosokawa. This would have been obvious because one of ordinary skill in the art would have been motivated to employ methods that are logical and have been known to be feasible in prior art technology.

Regarding claims 24, 26, 27, and 29, they are the system means and computer program product claims implementing the method of claims 21 and 23, and they are rejected, at least, for the same reasons.